William J. Pinilis
KAPLAN FOX & KILSHEIMER LLP
160 Morris Street
Morristown, NJ 07960
Telephone: (973) 656-0222
Facsimile: (973) 401-1114
wpinilis@kaplanfox.com

Joel B. Strauss
Peter S. Linden*
KAPLAN FOX & KILSHEIMER LLP
800 Third Avenue, 38th Floor
New York, NY 10022
Telephone: 212-687-1980
Facsimile: 212-687-7714
jstrauss@kaplanfox.com
plinden@kaplanfox.com

Joseph J. DePalma
Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

[Additional Plaintiff's Counsel on Signature Page]

Attorneys for Plaintiff and the Proposed Plaintiff Class

**Pro Hac Vice* applications forthcoming

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JESSICA FENN, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

HEALTHEC, LLC,

Defendant.

Case No.

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Jessica Fenn ("Plaintiff"), by and through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant HealthEC, LLC ("HEC" or "Defendant"), and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. HEC, a New Jersey company, is a nationwide healthcare technology company that styles itself as a "population health technology company that provides services to other entities."[1]

2. HEC states that it services clients in 18 States, boasting that "health organizations of all sizes trust HEC to help them meet the value-based-care commitments that they've made to their patients, the payers and their constituents."[2] In particular, it claims to service providers, payors and government entities, including over 1 million healthcare professionals, over 8 million members and payors and over 1,400 regional and national payors.[3]

3. In fulfilling its mission, HEC purports to "**deliver[] fully integrated analytics and insights** that enable value-based health systems and care organizations **to identify high-risk patients, close care gaps and recognize barriers** to optimal care."[4] HEC represents that: "Our data agnostic, AI-enabled solution ingests all available data — integrating clinical with claims data to create a community health record for each patient."[5]

4. In providing its services to its customers ("HEC Business Partners" or "Business Partners"), including healthcare professionals, payors and governmental entities, HEC "ingests"

[1] https://www.healthec.com/cyber-incident/
[2] https://www.healthec.com
[3] *Id.*
[4] https://www.healthec.com/ (Emphasis in original).
[5] *Id.*

and stores the personally identifiable information ("PII") and protected health information ("PHI")[6] of Business Partners' patients and clients, including those of Plaintiff and other members of the putative Class alleged herein (hereinafter, "Class Members"). This data includes highly sensitive and personal information such as clinical data, claims data, social security numbers, as well as Medicare, insurance and payment information. As such, HEC had a duty to maintain that data with the utmost care. Indeed, in a recent communication to plaintiff and Class Members, HEC admitted that "[w]e take … your privacy, and the security of information in our care very seriously."[7]

5. Upon information and belief, HEC's AI-enable system was especially vulnerable to compromise and security incidents. That security incident came to fruition between July 14, 2023 and July 23, 2023 when an unknown and unauthorized third party actor(s) gained access to HEC's system and copied the data of millions of persons whose PII and/or PHI was stored on HEC's system (the "Data Breach").[8]

6. It was not until December 22, 2023, more than five months later, that HEC announced the existence of the Data Breach in a "Notice of the HealthEC LLC Cyber Security Event" published on its website ("HEC Notice") and began notifying HEC Business Partners' patients of the Data Breach.[9]

7. Companies and governmental entities that were affected by the Data Breach include HEC Business Partners located throughout the United States. According to the HEC Notice, its "impacted business partners include Corewell Health, HonorHealth, University Medical Center of Princeton Physicians' Organization, Community Health Care Systems, State of Tennessee,

[6] As defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").
[7] https://www.healthec.com/cyber-incident/
[8] *Id.*
[9] *Id.*

Division of TennCare, Beaumont ACO, KidneyLink, Alliance for Integrated Care of New York, LLC, Compassion Health Care, Metro Community Health Centers, Advantage Care Diagnostic & Treatment Center, Inc., Long Island Select Healthcare, Mid Florida Hematology & Oncology Centers, P.A, d/b/a Mid-Florida Cancer Centers, Illinois Heath Practice Alliance, LLC, East Georgia Healthcare Center, Hudson Valley Regional Community Health Centers, and Upstate Family Health Center, Inc."[10]

8. The HEC Notice also explained that the Data Breach involved numerous types of information including name, address, date of birth, Social Security number, Taxpayer Identification number, Medical Record number, Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location), Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (including but not limited to patient account number, patient identification number, and treatment cost information) (collectively "Personally Identifiable Information" or "PII" and/or "Personally Identifiable Health Information" or "PHI").[11]

9. Upon information and belief, Defendant was aware, or should have been aware, of the data security shortcomings in its system. Nevertheless, HEC continued to use its systems to service HEC Business Partners and to store their customers' PII and PHI, putting those persons at risk of being impacted by a breach.

10. In particular, because HEC provided its services using AI technology it was subject to heightened cybersecurity risks. As such, it was obliged to take special precautions to avoid the type of data breach to which its business partners' customers have now been subjected.

[10] *Id.*
[11] *See* https://www.healthec.com/cyber-incident/

11. Upon information and belief, in order to obtain healthcare services from the various HEC Business Partners, Plaintiff and Class members (current and former patients, clients, or customers of HEC Business Partners) are required to provide sensitive, non-public PII and PHI to those Business Partners and entrust their highly sensitive data to such Business Partners and their agents for use and safekeeping. Defendant in turn collects and maintains this data and without such data could not perform its regular business activities. Defendant retains this information for many years and derives a benefit from the collection, maintenance and use of this data. As such, HEC had a duty to protect and safeguard this PII and PHI data from abuse and unauthorized access and use.

12. Defendant HEC's failure to ensure that its services were adequately secure fell far short of HEC's obligations and duties under State and Federal law, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"). Accordingly, HEC has jeopardized the security of the PII/PHI of Plaintiff and Class Members and has put them at serious risk of fraud and identity theft. Indeed, Plaintiff has already been informed by HEC that certain of her PII and PHI information has been impacted by the Data Breach.

13. HEC also failed to ensure that Plaintiff's and Class Members' reasonable expectations for data privacy would be maintained, jeopardizing the security of their PII/PHI and putting them at serious risk of fraud and identity theft, by failing to adequately maintain the security of Plaintiff's and Class Members' PII/PHI or upgrading its technology given HEC's knowledge of the risks associated with collecting and maintaining such personal and sensitive information.

14. Plaintiff brings this putative class action alleging that Defendant's conduct, as described more fully herein, caused Plaintiff's and other Class Members' PII and/or PHI to be

exposed and stolen because Defendant failed to safeguard and protect their sensitive information. Plaintiff seeks damages, and injunctive and other relief, on behalf of herself and similarly situated consumers.

PARTIES

15. Plaintiff Jessica Fenn is a resident of Wayne County, Michigan. She received a notice letter from HEC dated December 22, 2023 stating that her PHI/PII, including her name, date of birth, medical information and billing or claims information was compromised by the Data Breach. Additional allegations concerning Plaintiff's experience are set forth below.

16. Defendant Health EC, LLC ("HEC") is a limited liability company formed under the state laws of Delaware, with its principal place of business located at 343 Thornall Street, Suite #630, Edison, NJ 08837.

JURISDICTION AND VENUE

17. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

18. This Court has personal jurisdiction over HEC because it operates and maintains its principal place of business in this District. HEC is headquartered in New Jersey, is authorized to do business and does conduct business in New Jersey, has made substantial sales of its technology services from New Jersey and this District, and has sufficient minimum contacts with this state and/or sufficiently avail themselves of the markets and benefits of this state through its

promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

19. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant does substantial business in this District, maintains Plaintiff's and class members' PII and/or PHI in this District, has intentionally availed itself of the laws and markets within this District through its promotion, marketing, distribution and sales activities in this District, and a significant portion of the facts and circumstances giving rise to Plaintiff's Complaint occurred in or emanated from this District.

FACTUAL ALLEGATIONS

A. Background

20. HEC is a "population health technology company that provides services to other entities,"[12] offering an AI-enabled population health management platform to its Business Partners, which are comprised of 26 clients in located in 18 States.

21. HEC Business Partners include providers (such as accountable care organizations, primary care associations, community health centers, hospitals and health systems), payors (including Medicare advantage plans, Medicaid managed care organizations, and employer health plans) and government entities (State Medicaid agencies and Community health centers).

22. Through these Business Partners, HEC also provides technology services to their customers and patients, including over 1 million healthcare professionals, over 8 million members and payors and over 1,400 regional and national payors. *Id.*

23. In order to obtain healthcare from the various HEC Business Partners, Plaintiff and Class Members, who are current and former patients, clients and customers of HEC Business

[12] https://www.healthec.com/cyber-incident/

Partners, are required to provide sensitive, non-public PII and PHI to those Business Partners. Accordingly, Plaintiff and Class members entrust their highly sensitive data to such Business Partners and their agents, like HEC, for use and safekeeping. Defendant in turn collects this data from its Business Partners and maintains and stores this data. Without such data, HEC could not perform its regular business activities.

24. HEC's platform and technology services are used by HEC to collect data from its Business Partners, and then store, secure, and allow the use of Plaintiff's and Class Members' PII and PHI, the most sensitive and confidential type of information. Defendant retains this information for many years and derives a benefit from the collection, maintenance and use of this data. As such, HEC had a duty to protect and safeguard this PII and PHI data from abuse and unauthorized access and use.

B. HEC's Technology and Representations Regarding It

25. Plaintiff and Class Members relied on their healthcare providers and in turn their providers' vendor, HEC, to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

26. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII/PHI from involuntary disclosures to third parties.

27. In addition, the very nature of the technology HEC employed promised security. But in reality posed a heightened risk to the PII and PHI data it had collected.

28. In a 2019 HEC promotional article, it explained it approach:

> HealthEC, LLC, is the 2019 Best in KLAS®, full-service PHM [population health management] company with expertise in value-based care strategies, healthcare operations and workflows, outcomes measurement, provider performance monitoring, member management, and cutting-edge technology. Our mission is to

> help clients succeed through the use of our industry-leading, single-platform solution that aggregates and analyzes clinical, claims, and quality data to provide actionable insights that can improve healthcare outcomes across multiple dimensions.[13]

29. HEC also asserted that its platform was beneficial in detecting and identifying, and presumably preventing, abuse and promoting integrity:

> Our platform provides the ability to scan and detect unusual patterns and outliers to **help identify** waste and **abuse**, **report on program integrity**, and facilitate overall cost containment.[14]

30. HEC says that it "delivers fully integrated analytics and insights that enable value-based health systems and care organizations to identify high-risk patients, close care gaps and recognize barriers to optimal care."[15] HEC explains: "Our data agnostic, AI-enabled solution ingests all available data — integrating clinical with claims data to create a community health record for each patient." *Id.*

31. Given that it uses AI solutions, HEC was aware or should have been aware that the use of AI greatly increases the risk of cybersecurity threats. In particular:

> The advent of AI in this scenario has quickly become an exponential multiplier of threats poised to exploit and magnify existing cybersecurity gaps.
>
> While AI is a boon to enhance cybersecurity defenses, it also equips cybercriminals with more highly sophisticated tools. This dichotomy presents a unique challenge; the very technology meant to safeguard data can also be its biggest threat. Business and technology leaders, perhaps buoyed by overconfidence in existing security measures, have overlooked AI's potential for harm.[16]

---

[13] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWNbgF
[14] *Id.* (emphasis added).
[15] https://www.healthec.com
[16] https://www.securitymagazine.com/articles/100294-ai-driven-cyber-threats-require-saas-data-protection (Jan. 25, 2024 article in Security)

C. The Data Breach

32. On December 22, 2023, HEC published the HEC Notice that indicated at some undisclosed prior time, HEC "became aware of suspicious activity potentially involving its network."[17]

33. The HEC Notice also stated that it "promptly began an investigation."[18] However, HEC has not disclosed when or how it first learned of the suspicious activity.

34. The HEC Notice further explained that the "investigation determined that certain systems were accessed by an unknown actor between July 14, 2023 and July 23, 2023, and during this time certain files were copied."[19]

35. The HEC Notice also reported that after learning of the Data Breach it undertook a review of the files to identify "what specific information was present and to whom it relates" and that such "review was completed on or around October 24, 2023."[20]

36. It was not until the week of January 2, 2024, that the extent of the Data Breach was known.[21] At that time, the U.S. Department of Health and Human Services' breach portal reported that 4,452,782 individuals had been impacted by the Data Breach.[22]

D. Notification of HEC Customers

37. The HEC Notice indicated that HEC "began notifying our clients on October 26, 2023."[23] However, HEC did not begin to send notices out to Plaintiff and the millions of other

[17] https://www.healthec.com/cyber-incident/
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] https://www.scmagazine.com/news/healthec-hack-exposed-4-5m-patient-records-from-18-providers
[22] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[23] https://www.healthec.com/cyber-incident/

Class Members whose PHI and PII was exposed until almost two months later, on December 22, 2023.

38. On December 22, 2023, HEC began sending to Plaintiff, and upon information and belief, to other Class Members impacted by the Data Breach a letter notifying them about the Data Breach (hereinafter, the "Notice Letter"). For her part, during the week of January 2, 2024, Plaintiff received a form of the Notice Letter from HEC (the "Fenn Notice"), which was dated December 22, 2023.

39. Among other things the Fenn Notice stated:

> **What Happened?** HealthEC became aware of suspicious activity potentially involving our network and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023 and July 23, 2023, and during this time certain files were copied. We then undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it relates. This review identified information relating to some of our clients. We began notifying our clients on October 26, 2023, and we worked with them to notify potentially impacted individuals, including you. The organization on whose behalf HealthEC is providing your notice is Beaumont ACO.
>
> **What Information was Involved?** Your name and Date of Birth, Medical Information And Billing Or Claims Information were present in the impacted files.

40. Numerous companies and institutions, including certain State entities, across the U.S. (as well as almost 4.5 million of their patients, clients and customers) were affected by the Data Breach:

> **What HEC Business Partners/Customers are Impacted by this Event?** HealthEC's impacted business partners include Corewell Health, HonorHealth, University Medical Center of Princeton Physicians' Organization, Community Health Care Systems, State of Tennessee, Division of TennCare, Beaumont ACO, KidneyLink, Alliance for Integrated Care of New York, LLC, Compassion Health Care, Metro Community Health Centers, Advantage Care Diagnostic & Treatment Center, Inc., Long Island Select Healthcare, Mid Florida Hematology & Oncology Centers, P.A, d/b/a Mid-Florida Cancer Centers, Illinois Heath Practice Alliance,

LLC, East Georgia Healthcare Center, Hudson Valley Regional Community Health Centers, and Upstate Family Health Center, Inc.[24]

41. In the notice sent to Plaintiff and, upon information and belief, the other notice letters sent to Class members, HEC stated: "As an added precaution, we are offering twelve (12) months of credit monitoring and identity restoration services through TransUnion."[25]

42. On December 26, 2023, the Michigan Attorney General issued its own notice about the Data Breach and similarly reported that "HealthEC is offering 12 months of credit monitoring and identity protection services through TransUnion. Information on how to enroll will be mailed directly to potentially impacted patients."[26]

43. As explained below, given the harm caused by the Data Breach to Plaintiff and the millions of other Class Members, as well as the continued risk, HEC's "offer" is wholly inadequate to address the harm its Data Breach has caused.

E. Impact of the Data Breach

44. The Data Breach creates a heightened security concern for Plaintiff and Class Members because their PII and PHI, including unique medical records and other sensitive health and prescription information was included.

45. Medical privacy is among the most important tenets of American healthcare. Patients must be able to trust their physicians, insurers, and pharmacies to protect their medical information from improper disclosure including, but not limited to, their health conditions and

[24] *See* HEC Notice, dated Dec. 22, 2023, posted on HealthEC website: https://www.healthec.com/cyber-incident/
[25] *Id.*
[26] https://www.michigan.gov/ag/news/press-releases/2023/12/26/second-corewell-health-data-breach-exposes-info-of-one-million-michigan-patients

courses of treatment. Indeed, numerous state and federal laws require this. And, these laws are especially important when protecting individuals with particular medical conditions.

46. The Privacy Rule and Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandate the protection of and security for an individual's protected health information.[27]

47. Accordingly, the exposure of Plaintiff and Class Members' PHI through the Data Breach constitute a significant harm to these persons.

48. The theft of billing and claims information also harms victims, like Plaintiff and Class Members here, in a very significant manner.

49. The theft of billing information alone poses a significant risk that a Class Member's credit will be impaired and that the Class Member could be liable for any charges billed in her name. Indeed, the costs of *undoing* any impairment to a person's credit is itself a significant harm, which will take time and expense to reverse, repair or remediate.

50. The additional exposure of medical information exacerbates the harm greatly:

> "The majority of victims find out when they're trying to move on with their lives, if bills have gone to collections," says Eva Velasquez, president and CEO of the Identity Theft Resource Center, a nonprofit that provides free assistance to victims of identity theft. Someone may apply for a mortgage, for example, and learn their credit is ruined due to unpaid medical bills for care they didn't receive.
>
> **It's a double whammy. Unlike other forms of identity fraud, medical identity thieves may steal not only their victims' personal data — Social Security number, date of birth, address — but also information about their medical records and care, potentially putting their health at risk.**

[27] *See* HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule, 45 C.F. R. Part 160 and 164, Subparts A and C; *see also* https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

> "Sometimes people can't get their prescriptions, if their records are mixed with someone else's," Velasquez says. "Maybe you won't be able to get treatment that you need. There are serious implications."[28]

51. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. Indeed, the Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[29]

52. It is also difficult to obtain a new Social Security number. A breach victim would have to demonstrate ongoing harm from misuse of her Social Security number, and a new Social Security number will not be provided until after the victim has already suffered harm.

53. Given the highly sensitive nature of Social Security numbers, theft of these numbers in combination with other personally identifying information may cause damage to victims for years.

54. Defendant had a duty to keep PII/PHI confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their PII/PHI to their healthcare providers, with the understanding that their providers and their vendor would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

---

[28] Michelle Andrews, *Someone could steal your medical records and bill you for their care*, NPR, https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself (July 26, 2023) (emphasis added).

[29] *Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 12, 2024).

55. Defendant's data security obligations were particularly important given the substantial increases in data breaches in recent years, which are widely known to the public and to anyone in HEC's industry of data collection and transfer.

56. Data breaches are not new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks. Indeed, healthcare businesses such as Anthem and Premera Blue Cross have been subject to numerous data security incidents.

57. It is well known among companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals.

58. Identify theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

59. There may be a time lag between when the harm occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used. According, to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

60. With access to an individual's PII/PHI, criminals can commit all manners of fraud, including obtaining a driver's license or official identification card in the victim's name but with

[30] *Report to Congressional Requesters*, U.S. Government Accountability Office, (June 2007), http://www.gao.gov/new.items/d07737.pdf.

the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information.

61. PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers and other PII/PHI directly on various illegal websites making the information publicly available, often for a price.

62. Moreover, a study found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[31]

63. HEC is, and at all relevant times has been, aware that the sensitive PII/PHI it handles and stores in connection with providing its file transfer services is highly sensitive. As a company that provides technology services to collect and store data, involving highly sensitive and identifying information, HEC is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

64. HEC was aware, or should have been aware, of regulatory and industry guidance regarding data security.

65. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached, leaving its clients and all persons who provide sensitive PII/PHI to its clients exposed to risk of fraud and identity theft.

---

[31] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010, 5:00 a.m.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims; *see also* Annie Nova, *Here's how to avoid medical identity theft*, CNBC, (June 7, 2019 11:15 a.m.), https://www.cnbc.com/2019/06/07/how-to-avoid-medical-identity-theft.html.

66. The security flaws inherent to HEC's platform—and continuing to market and sell a platform with known, uncured security issues—run afoul of industry best practices and standards. Had HEC adequately protected and secured its platform, or stopped supporting the product when it learned about its vulnerabilities, it could have prevented the Data Breach.

67. Because HEC employed AI technology in its platform, it was aware, or should have been aware, that it was further at risk of being subject to a data breach.

68. Despite the fact that Defendant was on notice of the possibility of data theft associated with the HEC platform, it failed to make necessary changes to its technology or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the HEC platform's disclosure of Plaintiff's and Class members' PII/PHI to criminals.

69. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; disclosure of their medical conditions and courses of treatment; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PII/PHI; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of PII/PHI.

70. As a result of HEC's failure to ensure that its platform and other technology were protected and secured, or to enhance or to phase out the platform upon learning of its vulnerabilities, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their PII/PHI is now in the hands of criminals, they face a

substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PLAINTIFF'S EXPERIENCES

71. Plaintiff Jessica Fenn, a resident of Michigan, learned of the Data Breach via a Notice Letter that she received from HEC some time after January 1, 2024.

72. Plaintiff Jessica Fenn has been a patient at Grosse Pointe Beaumont Hospital, now known as St. John Ascension, which are part of Beaumont ACO, since approximately 2018.

73. As a result of learning of the Data Breach, Plaintiff has and will spend time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, retaining counsel, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts.

74. Plaintiff suffered actual injury in the form of damages to and diminution of the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of obtaining medical care, which was compromised in and as a result of the Data Breach.

75. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

76. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from the Data Breach, especially exposure of her insurance identification number and medical information, in combination with other PII/PHI, being placed in the hands of unauthorized third parties and criminals.

77. Plaintiff has a continued interest in ensuring that her PII/PHI, which remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

78. Plaintiff brings a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and all members of the following nationwide class (the "Class"):

> All persons in the United States whose PII/PHI was exposed to unauthorized third parties as a result of the compromise of HEC's platform that occurred between July 14, 2023 and July 23, 2023 (the "Class").

Plaintiff reserves the right to modify, change, or expand the Class definition, including proposing subclasses, based on discovery and further investigation.

79. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant have a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiff and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

80. The Class meet all of the criteria required by Federal Rule of Civil Procedure 23(a).

81. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it appears that the membership of the Class are in the tens of thousands, if not millions, of persons. The identities of Class members are also ascertainable through Defendant's records.

82. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether and to what extent Defendant had a duty to protect the PII/PHI of Plaintiff and Class Members;

(b) Whether Defendant failed to adequately safeguard the PII/PHI of Plaintiff and Class Members;

(c) Whether and when Defendant actually learned of the Data Breach;

(d) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII/PHI had been compromised;

(e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(f) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

(g) Whether Defendant were negligent or negligent per se;

(h) Whether Defendant violated the New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, *et seq.*;

(i) Whether Plaintiff and Class Members are entitled to relief from Defendant as a result of Defendant's misconduct, and if so, in what amounts; and

(j) Whether Class members are entitled to injunctive and/or declaratory relief to address the imminent and ongoing harm faced as a result of the Data Breach.

83. **Typicality:** Plaintiff's claims are typical of the claims of the Class they seek to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same misconduct alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

84. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class and has retained attorneys well experienced in class actions and complex litigation as their counsel,

including cases alleging breach of privacy and negligence claims arising from corporate misconduct.

85. The Class also satisfy the criteria for certification under Federal Rule of Civil Procedure 23(b) and 23(c). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendant have acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff also avers that certification of one or more subClass or issues may be appropriate for certification under Federal Rule of Civil Procedure 23(c). Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

86. Plaintiff and other members of the Class have suffered damages as a result of Defendant's unlawful and wrongful conduct. Absent a class action, Defendant's unlawful and improper conduct shall, in large measure, not go remedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further losses.

CLAIMS FOR RELIEF
COUNT I
Negligence

87. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

88. HEC negligently provided its platform and data management services which it knew or should have known were vulnerable to security breaches, despite representing that its technology would avoid abuse and promote the integrity of the data.

89. Defendant was entrusted with, stored, and otherwise had access to the PII/PHI of Plaintiff and Class Members.

90. Defendant knew, or should have known, of the risks inherent to storing the PII/PHI of Plaintiff and Class Members, and to not ensuring that HEC's platform and related technology were secure. These risks were reasonably foreseeable to Defendant, because HEC was using AI technology which posed a higher risk of vulnerability and because HEC did not take sufficient precautions to guard against data breach attacks.

91. Defendant owed duties of care to Plaintiff and Class Members whose PII/PHI had been entrusted to it.

92. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security in connection with the sale, and use of its platform and the PII and PHI data contained therein. Defendant had a duty to safeguard Plaintiff's and Class Members' PII and to ensure that their systems and products adequately protected PII.

93. Defendant further breached its duties by failing to promptly notify Plaintiff and other Class Members of the Data Breach or to take sufficient steps to remedy the Data Breach.

94. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

95. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII/PHI.

96. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

97. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury, including but not limited to: (i) the risk of identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

98. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

99. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se

100. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

101. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendant had a duty to provide adequate data security practices, including in connection with its sale and provision of its technology services, to safeguard Plaintiff's and Class Members' PII/PHI.

102. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1302d, *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII/PHI.

103. Pursuant to the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. § 56:8-163 ("CSBDA"), and the Michigan Identity Theft Protection Act, M.C.L.A. 445.72, and other similar applicable State laws, Defendant had a duty to disclose the Data Breach following its discovery to the persons whose data was exposed in the most expedient time possible and without reasonable delay.

104. Pursuant to other state and federal laws requiring the confidentiality of PII/PHI, Defendant had a duty to implement reasonably safeguards to protect Plaintiff's and Class Members' PII/PHI.

105. Defendant breached its duties to Plaintiff and Class Members under the FTC Act HIPAA, among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of their platform and technology services in order to safeguard Plaintiff's and Class Members' PII/PHI.

106. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

107. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

108. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII/PHI.

109. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

110. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy

111. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

112. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in the PII/PHI that Defendant disclosed without authorization.

113. Defendant owed a duty to Plaintiff and Class Members to keep their PII/PHI confidential.

114. Defendant failed to protect, and released to unknown and unauthorized third parties, the PII/PHI of Plaintiff and Class Members.

115. By failing to keep Plaintiff's and Class Members' PII/PHI safe, knowingly utilizing the unsecure HEC platform, and disclosing PII/PHI to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly

offensive to a reasonable person; (ii) improperly using their PII/PHI properly obtained for a specific purpose for another purpose, or disclosing it to a third party; (iii) failing to adequately secure their PII/PHI from disclosure to unauthorized persons; and (iv) enabling the disclosure of Plaintiff's and Class Members' PII/PHI without consent.

116. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

117. Defendant knew, or acted with reckless disregard of the fact that, the HEC platform and technology was vulnerable to data breaches prior to the Data Beach.

118. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PII/PHI was unduly frustrated and thwarted, and caused damages to Plaintiff and Class Members.

119. In failing to protect Plaintiff's and Class Members' PII/PHI, and in disclosing Plaintiff's and Class Members' PII/PHI, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

120. Plaintiff seeks injunctive relief on behalf of Plaintiff and the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV
Breach of Confidence

121. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Class.

122. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

123. Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

124. Plaintiff and Class Members provided their PII/PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII/PHI to be disseminated to any unauthorized third parties.

125. Plaintiff and Class Members provided their PII/PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

126. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII/PHI with the understanding that PII/PHI would not be disclosed or disseminated to unauthorized third parties or to the public.

127. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII/PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

128. As a proximate result of such unauthorized disclosures, Plaintiff and Class Members suffered damages.

129. But for Defendant's disclosure of Plaintiff's and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been compromised, stolen, viewed, access, and used by unauthorized third parties.

130. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII/PHI. Defendant knew or should have known that its methods of accepting, storing, transmitting and using Plaintiff's and Class Members' PII/PHI was inadequate.

131. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury, including but not limited to: (i) the risk of identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

132. As a direct proximate result of such unauthorized disclosures, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Breach of Third Party Beneficiary to Contract

133. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

134. Plaintiff and Class Members provided their PII/PHI to HEC Business Partners, respectively, including Beaumont ACO, with the explicit and implicit understandings that Defendant would take precautions to protect that PII/PHI from unauthorized disclosure.

135. Upon information and belief, Defendant entered into substantially similar or identical contracts with its business partner clients, including Beaumont ACO, to provide technology support services for its clients' patients healthcare data, which included data security practices, procedures, and protocols that purported to be sufficient to safeguard the PII/PHI and maintain its integrity and security.

136. Plaintiff and the Class Members were the express beneficiary of such contracts because the contracts contemplated HEC's collection, receipt, security and use of Plaintiff and Class Members' PII and PHI. Indeed, the contracts were made and drafted expressly for their benefit, which was the primary objective of the contracting parties.

137. Any harm to Plaintiff and the Class Members was the direct and foreseeable consequence of any breaches to HEC's contracts with its business partners. Thus, HEC knew that a breach of the contracts would result in damages or other harm to Plaintiff and the Class Members.

138. Plaintiff and Class Members are intended third party beneficiaries of contracts between HEC and its Business Partner clients, including, without limitation, Beaumont ACO. Under the circumstances, recognition of a right to performance by Plaintiff and the Class Members

is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and the Class Members the benefit of the performance promised in the contracts. Plaintiff and Class Members provided their PII/PHI to Defendant's business partners with the explicit and implicit understandings that Defendant would take precautions to protect that PII/PHI from unauthorized disclosure.

139. Defendant breached these agreements, which directly and/or proximately caused Plaintiff and the Class Members to suffer substantial damages.

140. Accordingly, Plaintiff and Class Members are entitled to damages, restitution, disgorgement of profits and other relief in an amount to be proven at trial.

COUNT VI

Violation of the New Jersey Consumer Fraud Act (N.J.S.A. §§ 56:8-2, *et. seq.*)

141. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

142. The New Jersey Consumer Fraud Act, § 56:8-2, provides in pertinent part:

> The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice….

N.J.S.A. § 56:8-2 (hereinafter, the "CFA").

143. HEC, from New Jersey, sold and provided to its Business Partners, including without limitation Beaumont ACO, "merchandise" under the CFA, in the form of its platform and technology services for the collection, maintenance and use of its Business Partners' patients, customers and/or clients, including Plaintiff and the Class Members herein.

144. HEC used or employed "commercial practice[s] that [were] unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation" within the meaning of the CFA, in that Defendant's conduct, as described herein:

(a) breached its duties pursuant to the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1302d, *et seq.*, and other applicable state, federal and regulatory laws, to implement reasonable safeguards to protect Plaintiff's and Class Members' PII/PHI;

(b) failed to disclose the Data Breach in a timely manner in violation of the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. § 56:8-163 ("CSBDA"), and the Michigan Identity Theft Protection Act, M.C.L. § 445.72, and other similar State laws;

(c) mispresented that its platform and technology services were safe and would properly and adequately safeguard Plaintiff's and Class Members' PII and PHI, provide adequate data security from unauthorized data beaches, prevent the abuse of, and promote integrity of, that information;

(d) misrepresented and/or failed to disclose material facts including that HEC's platform and technology services were subject to a heightened risk of data breach through the use of AI technology;

(e) failed to implement and maintain reasonable measures to ensure privacy and security of Plaintiff's and Class Members' PII and PHI; and

(f) concealed and/or failed to disclose that it did not implement and maintain reasonable measures to ensure privacy and security of Plaintiff's and Class Members' PII and PHI;

145. With respect to HEC's concealment of, and failures to disclose, material information in the sale or provision of its platform and technology services, Defendant knew or

should have known that such non-disclosures were inadequate to maintain the security of Plaintiff and Class Members' PII and PHI that were in HEC's possession.

146. Plaintiff has standing to pursue this claim because they have been injured and have suffered an ascertainable loss, by virtue of the wrongful conduct alleged herein.

147. As a direct and proximate cause of Defendant's conduct, which constitutes violations of the CFA as alleged herein, Plaintiff and Class Members have been damaged and suffered ascertainable losses due to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

148. Defendant's affirmative acts or statements, and nondisclosures or concealments, of material fact, alleged herein to be violations of the CFA, were made with intent that Plaintiff and Class members rely on them in entrusting their PII and PHI to HEC and their healthcare providers for collection, maintenance and use.

149. Plaintiff and Class members had a reasonable expectation that their PII and PHI would be properly safeguarded based on HEC's acts, misstatements and nondisclosures, which expectation was not met.

150. Plaintiff and Class Members are thereby entitled to recover treble damages, and/or restitution and equitable relief, including disgorgement or ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, filing fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

COUNT VII
Violation of Michigan Consumer Protection Act (Mich. Comp. Laws Ann. §§ 445.901, *et seq.* ("MCPA"))

151. Plaintiff realleges each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of herself and any other Class members that are residents of Michigan.

152. The MCPA, § 445.901(1), prohibits "unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce [as] unlawful" through a variety of means. *Id.,* § 445.901(1)(a)-(kk).

153. As alleged herein, Defendant violated the following provisions of the MCPA, § 445.901(1):

> "(c) Representing that goods or services have . . . characteristics, ingredients, uses, benefits, or quantities that they do not have . . .";
>
> "(e) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another";
>
> "(s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer";
>
> "(bb) Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is"; and
>
> "(cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner."

154. Defendant's conduct constituting the unfair, unconscionable, deceptive acts or practices that violated these provisions of the MCPA include but are not limited to:

(a) breaching its duties pursuant to, and/or failing to disclose that it has breached its duties pursuant to, the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1302d, *et seq.*, and other applicable state, federal and regulatory laws, to implement reasonable safeguards to protect Plaintiff's and Class Members' PII/PHI;

(b) failing to disclose the Data Breach in a timely manner in violation of the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. § 56:8-163 ("CSBDA"), and the Michigan Identity Theft Protection Act, M.C.L. § 445.72, and other similar State laws;

(c) mispresenting that its platform and technology services were safe and would properly and adequately safeguard Plaintiff's and Class Members' PII and PHI, provide adequate data security from unauthorized data beaches, prevent the abuse of, and promote integrity of, that information;

(d) misrepresenting and/or failed to disclose material facts including that HEC's platform and technology services were subject to a heightened risk of data breach through the use of AI technology;

(e) failing to implement and maintain reasonable measures to ensure privacy and security of Plaintiff's and Class Members' PII and PHI; and

(f) concealing and/or failed to disclose that it did not implement and maintain reasonable measures to ensure privacy and security of Plaintiff's and Class Members' PII and PHI.

155. Defendant is engaged in, and their acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the

course of Defendant's business of marketing, offering for sale, and selling or providing services throughout the United States, including in the State of Michigan.

156. Defendant had knowledge, not known to Plaintiff and the Class Members, of material information regarding the deficiencies and flaws in its platform and technology services and that such platform and technology was at risk of a data breach by unauthorized actors. Defendant also had knowledge, not known to Plaintiff and Class Members, of the extent of the Data Breach once it occurred until Class members received belated notice of the Data Breach in January 2023.

157. Defendant's conduct complained of herein was material as it related to highly sensitive information and precluded Plaintiff and Class members form taking steps to protect themselves against a Data Breach of PII and PHI.

158. Plaintiff and Class Members reasonably relied on Defendant's affirmative acts or statements, and nondisclosures or concealments, of material fact, alleged herein to be violations of the MCPA, the truth of which they could not have discovered.

159. Plaintiff has standing to pursue this claim under MCPA, § 445.911.

160. Plaintiff and the Class members have been injured and have suffered an ascertainable loss, by virtue of the wrongful conduct alleged herein. In addition, as a direct and proximate cause of Defendant's conduct, which constitutes violations of the MCPA as alleged herein, Plaintiff and Class Members have been damaged and suffered ascertainable losses due to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) the continued risk to their PII/PHI, which may remain in Defendant's possession

and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

161. Plaintiff and Class members had a reasonable expectation that their PII and PHI would be properly safeguarded based on HEC's acts, misstatements and nondisclosures, which expectation was not met.

162. Plaintiff and Class Members are thereby entitled to recover damages, and/or restitution and equitable relief, including disgorgement or ill-gotten gains, refunds of monies, interest, reasonable attorneys' fees, filing fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

COUNT VIII
Declaratory Relief
28 U.S.C. § 2201

163. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

164. An actual controversy has arisen and now exists between Plaintiff and the putative Class on the one hand, and Defendant on the other, concerning Defendant's failure to protect Plaintiff's and Class Members' PII/PHI in accordance with applicable state and federal regulations and the agreements between the parties. Plaintiff and the Class Members contend that Defendant failed to maintain adequate and reasonable privacy practices to protect their PII/PHI while on the other hand, Defendant contend they have complied with applicable state and federal regulations and its agreements with Plaintiff and Class Members to protect their PII/PHI.

165. Accordingly, Plaintiff and Class Members entitled to and seek a judicial determination of whether Defendant have performed, and are performing, their statutory and contractual privacy practices and obligations necessary to protect and safeguard Plaintiff's and Class Members' PII/PHI from further unauthorized, access, use, and disclosure, or insecure disposal.

166. A judicial determination of the rights and responsibilities of the parties over Defendant's privacy practices is necessary and appropriate at this time so that: (1) that the rights of the Plaintiff and the Class may be determined with certainty for purposes of resolving this action; and (2) so that the Parties will have an understanding of Defendant's obligations in the future given its continuing legal obligations and ongoing relationships with Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and on behalf of the Class, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23 against Defendant, appointing Plaintiff as Class Representative of the Class, and her counsel as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATED: January 16, 2024

KAPLAN FOX & KILSHEIMER LLP

By: */s/ Joel B. Strauss*

Joel B. Strauss
Peter S. Linden (*pro hac vice* application forthcoming)
KAPLAN FOX & KILSHEIMER LLP
800 Third Avenue, 38th Floor
New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
jstrauss@kaplanfox.com
plinden@kaplanfox.com

William J. Pinilis
160 Morris Street
Morristown, NJ 07960
Telephone: (973) 656-0222
Facsimile: (973) 401-1114
wpinilis@kaplanfox.com

Laurence D. King (*pro hac vice* application forthcoming)
Matthew B. George
(*pro hac vice* application forthcoming)
1999 Harrison Street, Suite 1560
Oakland, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com

LITE DEPALMA GREENBERG & AFANADOR, LLC
Joseph J. DePalma
Catherine B. Derenze
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

Attorneys for Plaintiff and the Proposed Plaintiff Class

CERTIFICATION PURSUANT TO LOCAL CIVIL RULE 11.2

Pursuant to Local Civil Rule 11.2, I hereby certify that the matter in controversy is related to the following civil actions:

- *Bishop v. HealthEC LLC*; Case No. 24-cv-00146 (D.N.J.); filed January 9, 2024
- *Black v. HealthEC, LLC et al*; Civil Action No. 24-cv-00232 (D.N.J.); filed January 12, 2024
- *Dinning v. HealthEC LLC et al.*; Civil Action No. 24-cv-10071 (E.D. Mich.); filed January 9, 2024
- *Fielder et al v. HealthEC, LLC et al.*; Civil Action No. 24-cv-00031 (D.N.J.); filed January 3, 2024
- *Khirfan v. HealthEC, LLC*; Civil Action No. 24-cv-00148 (D.N.J.); filed January 9, 2024
- *Leeb v. HealthEC, LLC*; Civil Action No. 24-cv-00036 (D.N.J.); filed January 4, 2024
- *Lempinen v. HealthEC, LLC*; Civil Action No. 24-cv-00026 (D.N.J.); filed January 3, 2024
- *Marano v. HealthEC LLC*; Civil Action No. 24-cv-00153 (D.N.J.); filed January 9, 2024
- *Markowitz et al v. HealthEC, LLC*; Civil Action No. 24-cv-00172 (D.N.J.); filed January 10, 2024
- *Palmiter v. HealthEC LLC*; Civil Action No. 24-cv-00027 (D.N.J.); filed January 3, 2024
- *Randall v. HealthEC, LLC*; Civil Action No. Civil Action no: 24-cv-00087 (D.N.J.); filed January 5, 2024
- *Schroeder v. HealthEC, LLC*; Civil Action No. 24-cv-00096 (D.N.J.); filed January 5, 2024

I hereby certify that the following statements made by me are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment.

DATED: January 16, 2024

KAPLAN FOX & KILSHEIMER LLP

By: */s/ Joel B. Strauss*

Joel B. Strauss
Peter S. Linden (*pro hac vice* application forthcoming)
KAPLAN FOX & KILSHEIMER LLP
800 Third Avenue, 38th Floor

New York, NY 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
jstrauss@kaplanfox.com
plinden@kaplanfox.com

William J. Pinilis
160 Morris Street
Morristown, NJ 07960
Telephone: (973) 656-0222
Facsimile: (973) 401-1114
wpinilis@kaplanfox.com

Laurence D. King (*pro hac vice* application forthcoming)
Matthew B. George
(*pro hac vice* application forthcoming)
1999 Harrison Street, Suite 1560
Oakland, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com

LITE DEPALMA GREENBERG & AFANADOR, LLC
Joseph J. DePalma
Catherine B. Derenze
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

Attorneys for Plaintiff and the Proposed Plaintiff Class